Konfigurieren eines IPSec-Tunnels zwischen einer Cisco Secure PIX Firewall und einer Checkpoint NG Firewall

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Netzwerkdiagramm Konventionen Konfigurieren des PIX Konfigurieren des Prüfpunkts NG Überprüfen Überprüfen der PIX-Konfiguration Tunnel-Status auf Checkpoint NG anzeigen Fehlerbehebung Fehlerbehebung bei der PIX-Konfiguration Netzwerkzusammenfassung Checkpoint NG-Protokolle anzeigen Zugehörige Informationen

Einführung

Dieses Dokument veranschaulicht, wie ein IPsec-Tunnel mit vorinstallierten Schlüsseln konfiguriert wird, um zwischen zwei privaten Netzwerken zu kommunizieren. In diesem Beispiel sind die Kommunikationsnetzwerke das private 192.168.10.x-Netzwerk innerhalb der Cisco Secure PIX Firewall und das private 10.32.x.x-Netzwerk innerhalb der ^{CheckpointTM} Next Generation Firewall (NG).

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Der Datenverkehr von innerhalb des PIX und innerhalb des ^{CheckpointTMTM} NG ins Internet (dargestellt durch die Netzwerke 172.18.124.x) sollte vor Beginn dieser Konfiguration fließen.
- Benutzer sollten mit der IPsec-Aushandlung vertraut sein. Dieser Prozess kann in fünf Schritte

unterteilt werden, darunter zwei IKE-Phasen (Internet Key Exchange).Ein IPsec-Tunnel wird durch interessanten Datenverkehr initiiert. Datenverkehr gilt als interessant, wenn er zwischen den IPsec-Peers übertragen wird.In IKE Phase 1 handeln die IPsec-Peers die etablierte IKE Security Association (SA)-Richtlinie aus. Nach der Authentifizierung der Peers wird ein sicherer Tunnel mithilfe von Internet Security Association und Key Management Protocol (ISAKMP) erstellt.In IKE Phase 2 verwenden die IPsec-Peers den authentifizierten und sicheren Tunnel, um IPsec-SA-Transformationen auszuhandeln. Die Aushandlung der freigegebenen Richtlinie bestimmt, wie der IPsec-Tunnel eingerichtet wird.Der IPsec-Tunnel wird erstellt, und Daten werden zwischen den IPsec-Peers übertragen, basierend auf den in den IPsec-Transformationssätzen konfigurierten IPsec-Parametern.Der IPsec-Tunnel endet, wenn die IPsec-SAs gelöscht werden oder ihre Lebensdauer abläuft.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- PIX Softwareversion 6.2.1
- CheckpointTM NG-Firewall

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfigurieren des PIX

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

PIX-Konfiguration	

PIX Version 6.2(1) nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname PIXRTPVPN domain-name cisco.com fixup protocol ftp 21 fixup protocol http 80 fixup protocol h323 h225 1720 fixup protocol h323 ras 1718-1719 fixup protocol ils 389 fixup protocol rsh 514 fixup protocol rtsp 554 fixup protocol smtp 25 fixup protocol sqlnet 1521 fixup protocol sip 5060 fixup protocol skinny 2000 names !--- Interesting traffic to be encrypted to the Checkpoint™ NG. access-list 101 permit ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0 !--- Do not perform Network Address Translation (NAT) on traffic to the Checkpoint™ NG. access-list nonat permit ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0 pager lines 24 interface ethernet0 10baset interface ethernet1 10full mtu outside 1500 mtu inside 1500 ip address outside 172.18.124.158 255.255.255.0 ip address inside 192.168.10.1 255.255.255.0 ip audit info action alarm ip audit attack action alarm pdm history enable arp timeout 14400 global (outside) 1 interface !--- Do not perform NAT on traffic to the Checkpoint™ NG. nat (inside) 0 access-list nonat nat (inside) 1 0.0.0.0 0.0.0.0 0 0 route outside 0.0.0.0 0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius aaa-server LOCAL protocol local no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps floodguard enable !--- Permit all inbound IPsec authenticated cipher sessions. sysopt connection permit-ipsec no sysopt route dnat !--- Defines IPsec encryption and authentication algorithms. crypto ipsec transform-set rtptac esp-3des esp-md5-hmac !--- Defines crypto map. crypto map rtprules 10 ipsecisakmp crypto map rtprules 10 match address 101 crypto map rtprules 10 set peer 172.18.124.157

```
crypto map rtprules 10 set transform-set rtptac
!--- Apply crypto map on the outside interface. crypto
map rtprules interface outside
isakmp enable outside
!--- Defines pre-shared secret used for IKE
authentication. isakmp key ******* address
172.18.124.157 netmask 255.255.255.255
!--- Defines ISAKMP policy. isakmp policy 1
authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:089b038c8e0dbc38d8ce5ca72cf920a5
: end
```

Konfigurieren des Prüfpunkts NG

Netzwerkobjekte und -regeln werden auf dem ^{CheckpointTM} NG definiert, um die Richtlinie zu bilden, die sich auf die einzurichtende VPN-Konfiguration bezieht. Diese Richtlinie wird dann mithilfe des ^{CheckpointTM} NG Policy Editor installiert, um die ^{CheckpointTM} NG-Seite der Konfiguration abzuschließen.

 Erstellen Sie die beiden Netzwerkobjekte f
ür das Checkpoint-Netzwerk und das PIX-Firewall-Netzwerk, die den interessanten Datenverkehr verschl
üsseln.W
ählen Sie dazu Verwalten > Netzwerkobjekte und anschlie
ßend Neu > Netzwerk aus. Geben Sie die entsprechenden Netzwerkinformationen ein, und klicken Sie dann auf OK.Diese Beispiele zeigen eine Reihe von Netzwerkobjekten mit dem Namen CP_Inside (innerhalb des Netzwerks von ^{CheckpointTM} NG) und PIXINSIDE (innerhalb des Netzwerks von

Network Properti	es - CP_inside		<u>×</u>
General NAT			
<u>N</u> ame:	CP_inside		
IP <u>A</u> ddress:	0.32.0.0]	
Net <u>M</u> ask:	255.255.128.0]	
Comment:	PINSIDE		
Color:			
Broadcast a	ddress: I O N <u>o</u> t included]	
		-	
	OK Cancel	Help	

Network Prope	ties - PIXINSIDE		×
General NAT			
<u>N</u> ame:	PIXINSIDE		
IP <u>A</u> ddress:	192.168.10.0		
Net <u>M</u> ask:	255.255.255.0		
<u>C</u> omment:	Pixinside		
Cojor:			
Broadcas <u>I</u> ncluc	t address: ed <u>O</u> N <u>o</u> t included		
	OK Cancel	Help	

2. Erstellen Sie Workstation-Objekte für ^{CheckpointTM} NG und PIX. Wählen Sie dazu Verwalten > Netzwerkobjekte > Neu > Workstation aus.Beachten Sie, dass Sie das ^{CheckpointTM} NG-Workstation-Objekt verwenden können, das während der ersten ^{CheckpointTM} NG-Einrichtung erstellt wurde. Wählen Sie die Optionen aus, um die Workstation als Gateway und interoperables VPN-Gerät festzulegen, und klicken Sie dann auf OK.Diese Beispiele zeigen eine Reihe von Objekten, die als ciscocp (CheckpointTM NG) und PIX (PIX Firewall) bezeichnet werden.

Workstation Properties - o	ciscocp			×
Workstation Properties - o General Topology NAT VPN Authentication Management II - Advanced	ciscocp General Name: IP Address: Color: Type:	ciscocp 172.18.124.157 Checkpoint External IP C Host © Gateway	<u>G</u> et address	X
	Check Point	Products int products installed: Version NG ireWall-1 o-1 ver anagement Station	i 🔽 Get Version]]
	Object Managed Managed Secure Interr Communic	gement	al) xtemal) cocppvzfoa	
		ОК	Cancel	Help

Workstation Properties - I	PIX			X
General — Topology	General			
- NAT	<u>N</u> ame:	PIX		
- VPN - Advanced	IP <u>A</u> ddress:	172.18.124.158	<u>G</u> et address	
	Comment:	PIX Firewall		
	Color:			
	Туре:	⊂ <u>H</u> ost ⊂ Gate <u>w</u> ay		
	Check Point P	Products		
	Check Po	int products installed: Version NG	i 💌 Gej Version	
	□VPN-1 & F □FloodGate □Policy Ser □Managem	iireWall-1 1 ver ent Station	*	
	Object Manaç	gement		
	C Managed	by this Management Server (Intern	al)	
	C Managed	by another Management Server (E)	ktemal)	
	Interope	rable ⊻PN Device		
,		ОК	Cancel Help	

3. Wählen Sie Verwalten > Netzwerkobjekte > Bearbeiten, um das Fenster Workstation-Eigenschaften für die ^{CheckpointTM} NG-Workstation zu öffnen (in diesem Beispiel ciscocp).Wählen Sie Topology aus den Optionen links im Fenster aus, und wählen Sie dann das Netzwerk aus, das verschlüsselt werden soll. Klicken Sie auf Bearbeiten, um die Schnittstelleneigenschaften festzulegen.

Workstation Properties -	tiscocp				×
- General - Topology - NAT - VPN - Authentication - Management El-Advanced	Topology <u>Giet Interfaces</u> Name II E100B0 1 E100B1 1	P Address 0.32.50.50 72.18.124.157	Network Mask 255.255.128.0 255.255.255.0	IP Addresses behind CP_inside External	
	.▲dd	<u>Edit</u>	<u>R</u> emove	ihow	
	VPN Domain VPN Domain All IP Addresses <u>b</u> information. <u>Manually Defined</u>	Gateway ehind Gateway ba	ised on Topology	Show Show	
	Exportable for Sec	uRemote			
,			ок с	ancel Help	

4. Wählen Sie die Option aus, um die Workstation als intern festzulegen, und geben Sie dann die entsprechende IP-Adresse an. Klicken Sie auf **OK**.In dieser Konfiguration ist CP_inside das interne Netzwerk des ^{CheckpointTM} NG. Die hier gezeigten Topologieauswahl bezeichnen die Workstation als intern und geben die Adresse als CP_inside

Interface Properties	×
General Topology QoS	
Topology	-
External (leads out to the internet)	
Internal (leads to the local network)	
IP Addresses behind this interface:	
◯ <u>N</u> ot Defined	
O Network defined by the interface IP and Net Mask	
	-
Anti-Spoofing	_
Perform Anti-Spoofing based on interface topology	
Spoof Tracking: 🔿 N <u>o</u> ne 💿 Log 🔿 Alert	
OK Cancel Help	

5. Wählen Sie im Fenster Eigenschaften von Workstations die externe Schnittstelle in ^{CheckpointTM} NG aus, die zum Internet führt, und klicken Sie dann auf **Bearbeiten**, um die Schnittstelleneigenschaften festzulegen. Wählen Sie die Option aus, um die Topologie als extern festzulegen, und klicken Sie dann auf

Interface Properties 📉
General Topology QoS
Topology
External (leads out to the internet)
Internal (leads to the local network)
IP Addresses behind this interface:
C Not Defined
C Network defined by the interface IP and Net Mask
O Specific:
Anti-Spoofing
Perform Anti-Spooring based on interrace topology
Spoot Fracking: O None 💿 Log O Alert
OK Cancel Help

OK.

6. Wählen Sie im Fenster Workstation Properties (Workstation-Eigenschaften) des ^{CheckpointTM} NG aus den Optionen links im Fenster VPN und anschließend IKE-Parameter für Verschlüsselungs- und Authentifizierungsalgorithmen aus. Klicken Sie auf Bearbeiten, um die IKE-Eigenschaften zu konfigurieren.

Workstation Properties - o	iscocp			×
General Topology NAT VPN Authentication Management € Advanced	VPN Encryption schemes	set default <u>I</u> KE prop	erties	
	Nickname DN	Edit	rtificate Authority	

7. Konfigurieren Sie die IKE-Eigenschaften:Wählen Sie die Option für die 3DES-Verschlüsselung aus, damit die IKE-Eigenschaften mit dem Befehl isakmp policy # encryption 3des kompatibel sind.Wählen Sie die Option für MD5 aus, damit die IKE-Eigenschaften mit dem Befehl crypto isakmp policy # hash md5 kompatibel

IKE Properties	×
General	
Support key exchange encryption w	ith:
CAST	
Support authentication methods:	
✓ Pre-Shared Secret	Edit <u>S</u> ecrets
Public <u>K</u> ey Signatures	Specify
□ VPN-1 & FireWall-1 authenticat	ion for SecuRemote (Hybrid Mode)
	<u>A</u> dvanced
OK Car	ncel Help

8. Wählen Sie die Authentifizierungsoption für vorinstallierte Geheimnisse aus, und klicken Sie dann auf Edit Secrets (Geheimnisse bearbeiten), um den vorinstallierten Schlüssel als kompatibel mit dem PIX-Befehl isakmp-Schlüssel-Adresse für die Netzmaske der Adresse festzulegen. Klicken Sie auf Bearbeiten, um den Schlüssel wie hier gezeigt einzugeben, und klicken Sie auf Festlegen.

	Shar	ed Secret				×
	Г	Shared Secrets Li	st:			1
		Peer Name	Shared Se	ecret		
		PIX	****		<u>E</u> dit	
					<u>R</u> emove	
		Enter secret:	iscortp	Set		
OK.		ОК] Cano	cel	<u>H</u> elp	

9. Klicken Sie im IKE-Eigenschaftenfenster auf Erweitert... und ändern Sie diese Einstellungen:Deaktivieren Sie die Option f
ür den aggressiven Support-Modus.W
ählen Sie die Option zum Austausch von Support-Schl
üsseln f
ür Subnetze aus.Klicken Sie abschlie
ßend auf

Advanced IKE properties			×
Use <u>U</u> DP encapsulation			
Constant Differ Hallman and an	UDP VPN1_IPS	EC_encapsi 💌	
Support Diffie-Hellman groups		0 Kin	
	Group 2 (102	24 bit)	
	Group 5 (15	36 bit)	
Rekeying Parameters	·		
Renegotiate IKE security associal	tions	1440 🔅	Minutes
Renegotiate IPSEC Security asso	ciations every	3600 🚊	Seconds
🔲 Renegotiate IPSEC Security a	associations ever	ry 50000 🚊	KBytes
Misc			
Support IP compression for Se	ecureClient		
Support aggresive mode			
Support key exchange for <u>s</u> ub	onets		
	ancel	Help	
		Пеф	

10. Wählen Sie Verwalten > Netzwerkobjekte > Bearbeiten, um das Fenster Workstation-Eigenschaften für PIX zu öffnen. Wählen Sie Topology aus den Optionen auf der linken Seite des Fensters aus, um die VPN-Domäne manuell zu definieren. In dieser Konfiguration wird PIXINSIDE (innerhalb des PIX-Netzwerks) als VPN-Domäne definiert.

rkstation Properties - F	-IX			
General	Topology			
I opology NAT	<u>G</u> et Interfaces			
VPN Advanced	Name	IP Address	Network Mask	
	Add	C-66	Remove C	2hour
		Ealtree .	Hernove 7	371399
	Show all IPs behind	I Gateway		
	VPN Domain			
	 All IP Addresses <u>b</u> information. 	gehind Gateway ba	ased on Topology	Show
	Manually Defined		-	Show
	Exportable for Ser	cuRemote		

11. Wählen Sie **VPN** aus den Optionen links im Fenster aus, und wählen Sie anschließend IKE als Verschlüsselungsschema aus. Klicken Sie auf **Bearbeiten**, um die IKE-Eigenschaften zu konfigurieren.

Workstation Properties - I	PIX			×
General Topology NAT Advanced	VPN Encryption schemes Image: Constraint of the schemes Edit			
		OK	Cancel	Help

12. Konfigurieren Sie die IKE-Eigenschaften wie folgt:Wählen Sie die Option für die **3DES**-Verschlüsselung aus, damit die IKE-Eigenschaften mit dem Befehl **isakmp policy # encryption 3des** kompatibel sind.Wählen Sie die Option für **MD5 aus**, damit die IKE-Eigenschaften mit dem Befehl **crypto isakmp policy # hash md5** kompatibel

IKE Properties	×
General	
Support key exchange encryption with: -	Support data integrity with:
	✓ MD <u>5</u>
CAST	
	<u>I SHAT</u>
- Support authentication methods:	
Pre-Shared Secret E	dit <u>S</u> ecrets
Public Key Signatures Mat	ching Criteria
□ VPN-1 & FireWall-1 authentication f	or SecuRemote (Hybrid Mode)
-	
	<u>A</u> dvanced
OK Cancel	Help

sind.

13. Wählen Sie die Authentifizierungsoption f
ür vorinstallierte Geheimnisse aus, und klicken Sie dann auf Edit Secrets (Geheimnisse bearbeiten), um den vorinstallierten Schl
üssel als kompatibel mit dem PIX-Befehl isakmp-Schl
üssel-Adresse f
ür Netzmaske-Adresse festzulegen. Klicken Sie auf Bearbeiten, um den Schl
üssel einzugeben, und klicken Sie dann auf Festlegen,

Shar	ed Secret		×
۲ ⁹	Shared Secrets List: -		
	Peer Name	Shared Secret	
	ciscocp	****	<u>E</u> dit
	,		
		Cancel	Help

14. Klicken Sie im IKE-Eigenschaftenfenster auf Erweitert... und diese Einstellungen ändern.Wählen Sie die für IKE-Eigenschaften geeignete Diffie-Hellman-Gruppe aus.Deaktivieren Sie die Option für den aggressiven Support-Modus.Wählen Sie die Option zum Austausch von Support-Schlüsseln für Subnetze aus.Klicken Sie abschließend auf

Advanced IKE properties			×
Use UDP encapsulation			
Support Diffie-Hellman groups	UDP VPN1_IPS	EC_encapsi 🔽	
	Group 1 (768	3 bit) 24 bit)	
	Group 5 (153	36 bit)	
Rekeying Parameters			
Renegotiate IKE security associ	ations	1440 🗧	Minutes
Renegotiate IPSEC Security ass	ociations every	3600 🗧	Seconds
Renegotiate IPSEC Security	associations ever	y 50000 🚊	KBytes
Misc Support IP compression for S Support aggresive mode Support key exchange for <u>s</u> u	BecureClient Jonets		
ОК	Cancel	<u>H</u> elp	

15. Wählen Sie Regeln > Regeln hinzufügen > Oben, um die Verschlüsselungsregeln für die Richtlinie zu konfigurieren.Fügen Sie im Fenster Richtlinien-Editor eine Regel mit der Quelle CP_inside (innerhalb des Netzwerks des Checkpoint TM NG) und PIXINSIDE (innerhalb des Netzwerks des PIX) sowohl in der Quell- als auch in der Zielspalte ein. Legen Sie Werte für Service = Any, Action = Encrypt und Track = Log fest. Wenn Sie den Abschnitt Encrypt Action (Aktion verschlüsseln) der Regel hinzugefügt haben, klicken Sie mit der rechten Maustaste auf Aktion, und wählen Sie Eigenschaften bearbeiten aus.

CISCOCP - Check Point Policy Editor	- Standar	d							
File Edit View Manage Rules Policy Topology Search Window Help									
■● 米 白 翰 ● 整 注 典 ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■									
₽ @ @ 8 0 %	🗣 🚓 🐼 📴 🐥 🧭 🗣 🗰 Security - Standard 🧱 Address Translation - Standard 📓 QoS - Standard 🛍 Desktop Security - Standard								
Retwork Objects B Workstation	NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL		
	1		부 POINSIDE 부 CP_inside	🛪 Any	Edit prop	erties	🔃 Gaterway:		
-++ O_inside	2	+ CP_inside	* Any	🗙 Алу	🔂 acc	Sb(23)	Gateway:		
OSE Device					 accept drop reject 				
- 🎹 Group - 🕎 Logical Server					Client A	uth			
P. Address Range		a a ta sa	[.]	the second second	Session	Auth	•		
2 Dynamic Object	Nan	e	IP	Conment	Encrypt				
	Cisc PIX	ocp	172.10.1 172.18.1	24.157 Chedipoir 24.158 PDX Firetwo	al External I 🙆 Client E	ncrypt			
					Query Ci Clear Qu	ery			

16. Wenn IKE ausgewählt und hervorgehoben ist, klicken Sie auf

Encryption Properties			×
General			
Encryption <u>s</u> chemes defined: —			
<u>E</u> dit			
OK Ca	ncel H	elp	

Bearbeiten.

17. Ändern Sie im Fenster IKE-Eigenschaften die Eigenschaften so, dass sie mit den PIX-IPsec-Transformationen im Befehl crypto ipsec-transformation rtptac esp-3des esp-md5hmac übereinstimmen.Legen Sie die Option Transform auf Encryption + Data Integrity (ESP) fest, legen Sie den Verschlüsselungsalgorithmus auf 3DES fest, legen Sie die Datenintegrität auf MD5 fest, und legen Sie das zulässige Peer-Gateway so fest, dass es dem externen PIX-Gateway entspricht (hier als PIX bezeichnet). Klicken Sie auf

IKE Properties	
General	
Transform	
Encryption + Data Integrity	y (ESP)
🔿 Data Integrity Only (AH)	
Encryption Algorithm:	3DES 💌
<u>D</u> ata Integrity	MD5
<u>C</u> ompression method:	None
Allowed Peer Gateway:	PIX 🔽
□ <u>U</u> se Perfect Forward Secrecy	
Use DH <u>G</u> roup:	Group 1 (768 bit) 💌
Perform IP <u>P</u> ool NAT	
	ncel Help

 Nachdem Sie ^{CheckpointTM} NG konfiguriert haben, speichern Sie die Richtlinie, und wählen Sie **Policy > Install** aus, um sie zu



Im Installationsfenster werden beim Kompilieren der Richtlinie Fortschrittshinweise angezeigt.



das Installationsfenster anzeigt, dass die Richtlinieninstallation abgeschlossen ist. Klicken Sie auf **Schließen**, um den Vorgang

abzuschließen.

Install Policy

Standard.W: Security Policy Script generated into Standard.pf
Standard:
Compiled OK.
Installing VPN-1/FireWall-1 policy On: ciscocp ...
VPN-1/FireWall-1 policy installed successfully on ciscocp...
VPN-1/FireWall-1 policy Installation for all modules was successful

Dose

<u>Überprüfen</u>

Überprüfen der PIX-Konfiguration

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**. Initiieren Sie einen Ping von einem privaten Netzwerk zum anderen, um die Kommunikation zwischen den beiden privaten Netzwerken zu testen. In dieser Konfiguration wurde von der PIX-Seite (192.168.10.2) ein Ping an das interne ^{CheckpointTM} NG-Netzwerk (10.32.50.51) gesendet.

• show crypto isakmp sa: Zeigt alle aktuellen IKE-SAs in einem Peer an.

```
show crypto isakmp sa
 Total
        : 1
 Embryonic : 0
              dst
                                       src
                                                                state
                                                                          pending created
   172.18.124.157 172.18.124.158 QM_IDLE
                                                     0
                                                                1
• show crypto ipsec sa: Zeigt die von aktuellen SAs verwendeten Einstellungen an.
 PIX501A#show cry ipsec sa
 interface: outside
     Crypto map tag: rtprules, local addr. 172.18.124.158
    local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.32.0.0/255.255.128.0/0/0)
    current_peer: 172.18.124.157
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
     #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
     #send errors 1, #recv errors 0
      local crypto endpt.: 172.18.124.158, remote crypto endpt.: 172.18.124.157
      path mtu 1500, ipsec overhead 56, media mtu 1500
      current outbound spi: 6b15a355
      inbound esp sas:
       spi: 0xced238c7(3469883591)
         transform: esp-3des esp-md5-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 3, crypto map: rtprules
         sa timing: remaining key lifetime (k/sec): (4607998/27019)
         IV size: 8 bytes
         replay detection support: Y
      inbound ah sas:
      inbound pcp sas:
      outbound esp sas:
       spi: 0x6b15a355(1796580181)
         transform: esp-3des esp-md5-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 4, crypto map: rtprules
         sa timing: remaining key lifetime (k/sec): (4607998/27019)
         IV size: 8 bytes
         replay detection support: Y
      outbound ah sas:
      outbound pcp sas:
```

Tunnel-Status auf Checkpoint NG anzeigen

Öffnen Sie den Richtlinien-Editor, und wählen Sie **Fenster > Systemstatus** aus, um den Tunnelstatus anzuzeigen.

CISCOCP - Check Point System Status									
<u>File View Modules Products Tools Window H</u> elp									
) 🖸 🗉 🗛 🔢 🔦 🎫 🇞 📾 🚅 🎯 😪	}?								
Modules IP Address	VPN-1 Details								
	Status:	ок							
E ciscocp 172.18.124.157	Packets								
FireWall-1	Encrypted:	20							
FloodGate-1	Decrypted:	20							
Management	Errors								
SVN Foundation	Encryption errors:	0							
MEIN-1	Decryption errors:	0							
	IKE events errors:	0							
	Hardware								
	HW Vendor Name:	none							
	HW Status:	none							

Fehlerbehebung

Fehlerbehebung bei der PIX-Konfiguration

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie <u>vor der</u> Verwendung von **Debug-**Befehlen die <u>Informationen</u> zu <u>Debug-</u><u>Befehlen</u>.

Verwenden Sie diese Befehle, um Debugging auf der PIX-Firewall zu aktivieren.

- debug crypto engine Zeigt Debugmeldungen über Krypto Engines an, die Verschlüsselung und Entschlüsselung durchführen.
- debug crypto isakmp: Zeigt Meldungen über IKE-Ereignisse an.

```
VPN Peer: ISAKMP: Added new peer: ip:172.18.124.157 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.124.157 Ref cnt incremented to:1 Total VPN Peers:1
ISAKMP (0): beginning Main Mode exchange
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
```

```
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
ISAKMP (0): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated
ISAKMP (0): beginning Quick Mode exchange, M-ID of 322868148:133e93b4 IPSEC(key_engine): got a
queue event...
IPSEC(spi_response): getting spi 0xced238c7(3469883591) for SA
from 172.18.124.157 to 172.18.124.158 for prot 3
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
ISAKMP (0): sending INITIAL_CONTACT notify
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 322868148
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable. IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.158,
dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0): processing NONCE payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): Creating IPSec SAs
inbound SA from 172.18.124.157 to 172.18.124.158 (proxy 10.32.0.0 to 192.168.10.0)
has spi 3469883591 and conn_id 3 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 172.18.124.158 to 172.18.124.157 (proxy 192.168.10.0 to 10.32.0.0)
has spi 1796580181 and conn_id 4 and flags 4
```

lifetime of 28800 seconds lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 172.18.124.158, src= 172.18.124.157, dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), src_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0xced238c7(3469883591), conn_id= 3, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 172.18.124.158, dest= 172.18.124.157, src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0x6b15a355(1796580181), conn_id= 4, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:2 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:3 Total VPN Peers:1 return status is IKMP_NO_ERROR

Netzwerkzusammenfassung

Wenn mehrere benachbarte Netzwerke in der Verschlüsselungsdomäne am Checkpoint konfiguriert sind, kann das Gerät diese automatisch in Bezug auf interessanten Datenverkehr zusammenfassen. Wenn die Crypto Access Control List (ACL) auf dem PIX nicht für eine Übereinstimmung konfiguriert ist, schlägt der Tunnel wahrscheinlich fehl. Wenn beispielsweise die internen Netzwerke 10.0.0.0 /24 und 10.0.1.0 /24 so konfiguriert sind, dass sie in den Tunnel aufgenommen werden, können sie in 10.0.0.0 /23 zusammengefasst werden.

Checkpoint NG-Protokolle anzeigen

-T	C15COCP -	Check Poi	nt Log Vie	wer - [fw	.log]					ē-+};;;;}	11	
6k	jile Mode Edit Selection Yew Iooks Window Help											
é	9 🤹 🖏	Log		* 🗛	Ŧ±	۵ ک	B 5	📑 🗰 🛱	l 🇞 🔛 😘	80	Į.	
1	Date	Time	Product		Inter.	Orig	Туре	Action	Source	Destina		info.
0	23Aug200	2 17:32:47	VPN-1	8 Find/Val	l 💽 da.	. ciscoop	🔳 log	Ow key install	PDC	ciscocp		KE: Mein Mode completion.
t	23Aug200	2 17:32:47	VPN-4	8 Fire/Val	l 💽 de.	. ciscocp	📕 log	D-w key install	PX	ciscocp		IKE. Quick Mode Received Notification from Peer: Initial Contact
2	23Aug200	2 17:32:47	VPN-1	& Firel/Val	l 💽 da.	. ciecocp	🔳 log	Dre key install	PIX	ciscocp		IKE: Guick Mode completion IKE IDs: subnet: 10.32.0.0 (mosk= 255.25
з	23Aug200	2 17:32:48	VPN-1	& Firel/Val	L., 💽 🖬.,	ciscoop	🔳 log	😡 decrypt	192.168.10.2	10.32.50.51	0	ionp-type 0 ionp-code 0
4	23Aug200	2 17:32:48	器 VPN-1	& Fire/Val	🕞 E1.	. ciscoop	📕 log	🞑 decrypt	192.168.10.2	10.32.50.51	0	icmp-type 8 icmp-code 0
5	23Aug200	2 17:32:48	RE VEN-1	& Firel/Val	🕞 🛯	. clecoop	Iog	🔒 decrypt	192.168.10.2	10.32.50.51	0	icmp-type 0 icmp-code 0
6	23Aug200	2 17:32:48	VPN-1	& Fire/Val	📻 🛃	ciscoop	🗐 log	😡 decrypt	192.168.10.2	10.32.50.51	0	iomp-type 0 iomp-code 0

Wählen Sie Window > Log Viewer aus, um die Protokolle anzuzeigen.

Zugehörige Informationen

- <u>Cisco PIX Firewall-Software</u>
- <u>Cisco Secure PIX Firewall Befehlsreferenzen</u>
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation Cisco Systems